A group is a set together with an associative operation such that there is an identity, every element has an inverse and any pair of elements can be combined without going outside the set.

Examples. 1 $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ are groups. In each case the identity is 0 and the inverse of a is $-a$.

2. $(\mathbb{Z},\cdot)$ is not a group. The identity is 1 but there is no inverse of any element except 1.

3. The set $\{1,-1,i,-i\}$ of 4 complex numbers is a group under complex multiplication.

4. The set $\mathbb{Q}^+$ of positive rationals is a group under ordinary multiplication. The inverse of any a is $\frac{1}{a} = a^{-1}$.

5. The set of all 2x2 matrices with real entries is a group under addition.

6. The set $\mathbb{Z}_n = \{0,1,\dots,n-1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in $\mathbb{Z}_n$, the inverse of j is $n-j$. This group is usually referred to as the group of integers modulo n.

7. The set $\mathbb{R}^*$ of nonzero real numbers is a group under ordinary multiplication. The identity is 1. The inverse of a is $\frac{1}{a}$.

8. The set $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}$ of 2x2 matrices with real entries and nonzero determinant is a group under matrix multiplication. The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

9. let $R = \{r_0, r_{60}, r_{120}, r_{180}, r_{240}, r_{300}\}$ where r_θ denotes the rotation of geometric figures drawn on a plane by θ degrees. let $*$ be the operation defined as $r_{\theta_1} * r_{\theta_2} = r_{\theta_1+\theta_2}$. Then $(R, *)$ is a group. r_0 is the identity element and $r_{360-\theta}$ is the inverse of r_θ.

Abelian group: A group $(G, *)$ is called abelian group or commutative group if this group satisfies commutative law i.e. $\forall a, b \in G$; $a * b = b * a$.

Q. Let $U_n = \{0, 1, 2, \ldots, n-1\}$. Let $*$ be binary operation on U_n such that $a * b =$ the remainder of ab divided by n. This $*$ is denoted by $\otimes_n$ (multiplication modulo n). Show that $(U_n, \otimes)$ is a semigroup.

Soln:- Closure property: Let $a, b \in U_n$ and $a \times b = c$.

Then c is either $< n$ or $\geq n$.

If $c < n$ then $c \in U_n$.

If $c \geq n$ then by definition of $*$, divide c by n then remainder must be less than n. $\Rightarrow a * b \in U_n$

$\therefore$ Both cases, $a * b \in U_n$ or $a \otimes_n b \in U_n$.

Thus, $(U_n, \otimes_n)$ is an algebraic structure.

Associative property: let $a, b, c \in U_n$ be any elements.

Then to show $(a \otimes_n b) \otimes_n c = a \otimes_n (b \otimes_n c)$.

Let $(a \otimes_n b) = r_1$, $r_1 \otimes_n c = r_2$ [i.e. $(a \otimes_n b) \otimes_n c = r_2$]

$\therefore$ $ab = nq_1 + r_1$ (Divison Algo) — (i)

& $r_1 c = nq_2 + r_2$ (") — (ii)

By (i), $(ab)c = nq_1 c + r_1 c = nq_1 c + nq_2 + r_2$ (By (ii))

$= n(q_1 c + q_2) + r_2$

Let $(b \otimes_n c) = r_3$, $a \otimes_n r_3 = r_4$ [i.e. $(a \otimes_n (b \otimes_n c) = r_4$]

$\therefore$ $bc = nq_3 + r_3$ — (iii)

$ar_3 = nq_4 + r_4$ — (iv)

By (iii), $a(bc) = anq_3 + ar_3 = anq_3 + nq_4 + r_4 = n(aq_3 + q_4) + r_4$

Since $(ab)c = a(bc)$ then $r_2 = r_4$.

$\therefore$ $(a \otimes_n b) \otimes_n c = a \otimes_n (b \otimes_n c)$.

Hence, the A.S. $(U_n, \otimes_n)$ is a semigroup.

Cayley Table:

$\mathbb{Z}_4 = \{0, 1, 2, 3\}, \oplus_4$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

0 is the identity.
inverse of 0 = 0
" 1 = 3
" 2 = 2
" 3 = 1

$G = \{1, -1, i, -i\}, \times$

$\times$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	+1	-1

1 is the identity.
inverse of 1 = 1
" -1 = -1
" i = -i
" -i = +i

Every row or column contains each element exactly one time.

Order of the group: The number of elements of the group $(G, *)$ is called order of the group. So, it may be finite (i.e. n) or infinite (i.e. $|\mathbb{N}|$). It is denoted as $O(G)$ or $|G|$.

lemma: In a group G,

(1) Identity element is unique. (2) Inverse of each $a \in G$ is unique

(3) $(a^{-1})^{-1} = a$, $\forall a \in G$, where a^{-1} stands for inverse of a.

(4) $(ab)^{-1} = b^{-1}a^{-1}$ $\forall a, b \in G$ (5) $ab = ac \Rightarrow b = c$ | $ba = ca \Rightarrow b = c$ $\forall a, b, c \in G$

(Cancellation laws)